



Scott M. Kessler

Akerman LLP  
666 Fifth Avenue  
20th Floor  
New York, NY 10103  
Tel: 212.880.3800  
Fax: 212.880.8965

Dir: 212.880.3874  
Dir Fax: 212.905.6411  
Scott.Kessler@akerman.com

May 22, 2015

**VIA ECF**

The Honorable Loretta A. Preska, Chief U.S.D.J.  
United States Courthouse  
500 Pearl Street, Room 2220  
New York, NY 10007

**Re: KLX Inc. v. Nissen, et al.; Case No. 7:15 Civ. 2782 (LAP)**

Dear Judge Preska:

We represent Plaintiff KLX Inc. ("Plaintiff" or "KLX") in the above-caption matter and submit this pre-motion conference letter pursuant to Local Civil Rule 37.2 of the Southern District of New York. On May 22, 2015, counsel for the parties conducted a meet and confer but were unable to resolve the discovery dispute outlined below.

As this Court is aware, on May 14, 2015, Plaintiff's application for expedited discovery was granted and ordered. In light of the Court's Order and Defendants' position that the discovery requests served by Plaintiff on or about April 13, 2015 were premature, Plaintiff again served its discovery requests on Defendants on May 15, 2015. Specifically, Plaintiff, as set forth in Request No. 9 in Plaintiff's Requests for Production of Documents (annexed hereto as **Exhibit A**), to both David Nissen and Joan Nissen requested the inspection of:

Any computer hard drive; any computer; any computer diskette, CD ROM, or DVD; any removable media or external storage devices including, but not limited to, printers, zip drives, jump drives, cloud storage devices, flash drives, thumb drives, USB drives, or any other external drives; and any iPhone, Android, Blackberry, Palm Pilot, cellular telephone, tablet, or any electronic organizing and/or messaging device in your care custody or control on which Proprietary Information was viewed, stored, printed,

[akerman.com](http://akerman.com)

The Honorable Loretta A. Preska, Chief U.S.D.J.

May 22, 2015

Page 2

---

managed or accessed, at any time.

On May 20, 2015, Defendants demanded that Plaintiff withdraw this request and further objected to Requests No. 9 on the basis that "they are overly broad, unduly burdensome, overlapping and duplicative, vague and ambiguous with respect to the term 'Proprietary Information,' and not limited as to time. Defendants further object to the Requests on the basis that they seek information that is: (a) exempt from discovery under the attorney-client communications privilege, work product doctrine, joint defense privilege, self-evaluating privilege, or other privilege or exemption under applicable law; (b) neither relevant nor reasonably calculated to lead to the discovery of admissible evidence; and (c) outside the possession, custody or control of Defendants." *See Exhibit B*. Thus, Defendants have refused to permit Plaintiff to conduct a forensic analysis of their computers and devices despite there being no dispute that each Defendant **admittedly** sent highly confidential and sensitive KLX information to their personal email accounts while employed by KLX, and intended to competitively use such information after their employment with KLX ended. Exhibit C, Responses Nos. 1-4; Exhibit D, Responses Nos. 1-4 (which are Defendants' respective objections and responses to Plaintiff's First Request for Admissions). Further, one of the Defendants, David Nissen, claims to no longer be in possession of the information he stole, now alleging that he deleted all information from his email account prior to the commencement of this litigation.

Plaintiff responded that it will not withdraw Requests No. 9 because it must be permitted to determine the accuracy of Defendants' statements, the current location of the information transmitted by Defendants, and whether Defendants completed their objective of disseminating the information to any third parties, including their new employer, J&K Electronics, Inc. d/b/a M3 Technologies, Inc. ("M3 Tech"), a direct competitor of KLX. Defendants have provided no assurances that they will conduct an exhaustive and complete search for the information sought by Plaintiff, such as hidden files and fragments or in cloud storage/backup areas, nor have Defendants provided any information on the methodology they have used or will use to obtain documents and information in response to Plaintiff's discovery requests. *See, e.g., Genworth Fin. Wealth Mgmt., Inc. v. McMullan*, 267 F.R.D. 443, 447–48 (D. Conn. 2010) (finding sufficient nexus between claims and need for computer imaging where plaintiff alleged that defendant admittedly used personal computers to download and access plaintiff's confidential information); *Ameriwood Indus., Inc. v. Liberman*, 2006 WL 3825291, \*5 (E.D. Mo. 2006) (permitting imaging in trade secrets case where the plaintiff argued that defendants may have further transmitted to others or deleted to hide the defendants' actions). For such reasons, Plaintiff must be permitted to forensically review Defendants' computers and devices.

Moreover, prior to the Court's order directing expedited discovery, Plaintiff provided Defendants' counsel with an Electronically Stored Information ("ESI") Protocol wherein Defendants' counsel would be provided with a 72-hour period to review the results of any forensic analysis for privacy and privilege concerns. The parties also already executed, and the Court entered, a confidentiality agreement which included "Confidential" and "Highly Confidential" designations for documents or communications including any of Defendants'

The Honorable Loretta A. Preska, Chief U.S.D.J.

May 22, 2015

Page 3

---

personal information. Thus, after much negotiation, the parties largely reached an agreement on a procedure and terms for the ESI searches and forensic analysis, but were unable to agree on the final timeframe and scope.

During counsel's meet and confer, Plaintiff again reiterated that its formal request for a forensic review of Defendants' computers and other portable devices would be subject to the parameters of the proposed ESI Protocol so as to satisfy all of Defendants' privacy and privilege concerns. Nonetheless, Defendants have refused to provide their computer and other devices for review. Instead, Defendants expect Plaintiffs to rely on the unverified word of the very same Defendants who wrongfully transmitted, with intent to use, KLX's proprietary information to their personal email addresses, that they no longer possess this information or never transmitted the information to any third parties, including M3 Tech. As Judge Karas already found, Plaintiff established irreparable harm, including that Defendants: (a) indisputably stole KLX confidential information; and (b) did so under circumstances suggesting disclosure is inevitable, including that Defendants are likely to use such information to the benefit of their new employer, a direct competitor of KLX. Absent an order directing Defendants' immediate production and Plaintiff's immediate inspection of Defendants' computers and other devices, Plaintiff will be unable to identify the full scope of information disseminated and take further action to prevent any additional disclosure(s).

Based on the foregoing, Plaintiff requests that the Court enter an Order compelling Defendants to permit Plaintiff, through its vendor and subject to an agreed ESI Protocol, to forensically examine and analyze Defendants' computers and other identified portable devices.

Respectfully submitted,

*/s/ Scott M. Kessler*

Scott M. Kessler

cc: Norman R. Cerullo, Esq.  
Jennifer Hartmann, Esq.